

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-54 are pending in the present application. Claims 1, 4, 8-10, 12, 16, 17, 20, 24-26, 32, 33, 36, 40-42 and 48 have been amended, and new Claims 49-54 have been added without the introduction of any new matter.

In the outstanding Office Action, Claims 1-48 were rejected under 35 U.S.C. § 103(a) as unpatentable over DeBry (U.S. Patent No. 6,385,728) in view of Padgett et al. (U.S. Patent No. 6,535,978, herein "Padgett").

Claims 1-48 were rejected under 35 U.S.C. § 103(a) as unpatentable over DeBry in view of Padgett. That rejection is respectfully traversed.

Amended independent Claim 1 is directed to a method for authorizing an electronic data transfer for healthcare transactions that includes receiving an authentication request containing a digital certificate from a requesting device via a communication link, determining whether the digital certificate is valid, creating an authentication response, sending the authentication response to the requesting device via the communication link, and securely storing audit trail information about the electronic data transfer, the digital certificate and at least a portion of the authentication response in a database. Creating the authentication response includes denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid. Securely storing the audit trail information includes ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic data transfer may be established.

Amended independent claims 9, 17, 25, 33 and 41 also include authorizing an electronic data transfer for healthcare transactions that includes securely storing audit trail information about the electronic data transfer, the digital certificate and at least a portion of the authentication response. Securely storing the audit trail information includes ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic

data transfer may be established.

In a non-limiting example, Figures 1, 2 and 5 illustrate a system and method for authorizing (220 and 240) an electronic data transfer for healthcare transactions, such as a transaction relating to a doctor completed screen form 510. The system 100 includes one or more data repositories or vaults (150, 160 or 170) that store the audit trail information necessary to establish non-repudiation for data transfers (see also page 16, lines 17-19). Specifically, audit trail information is securely stored 250 such that the long-term data integrity and reliability of the audit trail information is ensured and non-repudiation of the electronic data transfer may be established. Applicants submit that the present invention addresses the verification, validation and non-repudiation requirement of HIPAA (see also page 15, lines 16 and 17). Non-repudiation (*e.g.*, “ensuring the long-term data integrity and reliability of the audit trail information”) means that there is a “legal grade” receipt that provides strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid (see also page 15, lines 17-20).

DeBry does not relate to healthcare transactions. Instead, DeBry relates to securely printing a file retrieved from a separate file source in a network environment (see col. 1, lines 29-33). Applicants submit that healthcare transactions are substantially different than securely printing files to a network printer. Further, DeBry does not teach or suggest authorizing an electronic data transfer for healthcare transactions that includes securely storing audit trail information about the electronic data transfer, the digital certificate and at least a portion of the authentication response in a database. DeBry further does not teach or suggest ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic data transfer may be established. Instead, DeBry discloses encryption for the purpose of transmitting data from a sender to a recipient (a printer). DeBry discloses a log file or database possibly used to determine whether an issued will-call certificate matches information in the received will-call certificate (see col. 8, lines 27-31). Unlike the present invention, DeBry does not disclose that the log file in anyway contains audit trail information, nor that the long-term data integrity and reliability of the data within the log file is in anyway ensured. In fact, DeBry does not even mention non-repudiation. DeBry thus does not teach or suggest ensuring the integrity of data over some period of time or encrypting data after it is transmitted.

Applicants submit that maintaining an unsecured log file for comparison purposes is fundamentally different than securely storing information as a legal grade receipt to be used for non-repudiation purposes (*i.e.*, ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic data transfer may be established).

Padgett generally discloses electronic authentication using biological indicia, such as chromosomal DNA, a photograph, scanned fingerprint, iris or retina (see Abstract; col. 2, lines 31-66). A digitized bio-blob is transmitted to a recipient is compared against a bio-blob stored in a bio-blob database that was previously registered by a registrant (see col. 5, line 62 to col. 6, line 42). Similar to DeBry, Padgett does not teach or suggest ensuring the long-term data integrity and reliability of audit trail information such that non-repudiation of the electronic data transfer may be established. Instead, Padgett merely discloses encryption for the purpose of transmitting data from a sender to a recipient. Padgett thus does not teach or suggest ensuring the integrity of data over some period of time or encrypting data after it is transmitted.

As stated in M.P.E.P. §2143, a basic requirement for a prima facie case of obviousness is that the prior art reference (or references when combined) must teach or suggest all the claim limitations. As the cited references do not teach or suggest the feature of authorizing an electronic data transfer for healthcare transactions that includes securely storing audit trail information about the electronic data transfer, the digital certificate and at least a portion of the authentication response in a database, nor ensuring the long-term data integrity and reliability of the audit trail information such that non-repudiation of the electronic data transfer may be established, it is respectfully submitted the outstanding Office Action has not created a prima facie case of obviousness with regard to the claims dependent from amended independent Claims 1, 9, 17, 25, 33 and 41.

Accordingly, it is respectfully requested this rejection be withdrawn.

Additionally, dependent Claims 4, 20 and 36 of the present invention further define over the applied art for the additional reason now discussed. Dependent Claims 4, 20 and 36 each recite that the authentication response includes a date/time stamp of the authentication. DeBry and Padgett do not teach or suggest a date/time stamp of the authentication itself. Instead, Padgett discloses a certificate expiration date (*i.e.*, “a date until which the certificate is valid.”)

(see col. 7, lines 28-30). Accordingly, the above-noted dependent claims even further distinguish over the applied art.

Finally, new dependent Claims 49-54 have been added without the introduction of any new matter. Applicants submit that new dependent Claims 49-54 distinguish over the applied art because the applied art does not disclose audit trail information that is encrypted and signed.

CONCLUSION

In light of the arguments set forth above, Applicants respectfully submit that the Application is now in allowable form. Accordingly, Applicants respectfully request consideration and allowance of the currently pending claims.

It is believed that no additional fees are due at this time. If this is incorrect, Applicants hereby authorize the Commissioner to charge any fees, other than issue fees, that may be required by this paper to Deposit Account No. 07-0153. The Examiner is respectfully requested to call Applicants' Attorney for any reason that would advance the current application to issue. Please reference Attorney Docket No. 124521-1000.

Dated: December 19, 2005

Respectfully submitted,

GARDERE WYNNE SEWELL LLP



Karl L. Larson
Registration No. 41,141

ATTORNEY FOR APPLICANTS

3000 Thanksgiving Tower
1601 Elm Street
Dallas, Texas 75201-4761
(214) 999-4582 - Telephone
(214) 999-3623- Facsimile